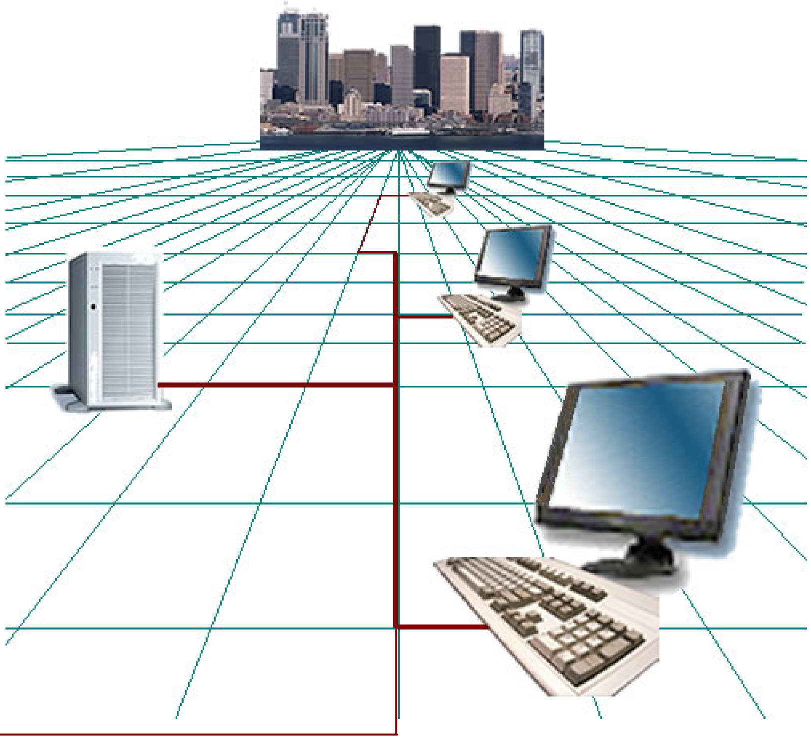
ADVANETRIX®, INC

Providing Targeted IT Solutions



Microsoft CERTIFIED Partner

www.advanetrix.com

Corporate Overview

Millennium Corporation was incorporated in the State of Virginia in 1997. Our initial focus was on providing unique Architecture Engineering and Technical support centered on the decision – maker. This focus integrated the Operational, Systems, and Technical Architectures to provide a complete systems engineering approach to analyzing Command, Control, Communications, Computers, and Intelligence (C^4I) systems, processes, procedures, and information flows.

In 1998, we became a Woman-Owned small business and began applying our C^4I skills to support our customers requiring Information Assurance services. We also expanded our training program to include an Information Assurance training module.

In 2000, we became a Microsoft Certified Solution Provider and began providing services to commercial organizations. During this time we also implemented a network training and certification program focused on integrating Microsoft products to provide customer-targeted solutions.

In 2002, Millennium Corporation became ADVANETRIX, Inc. The new name was chosen to more accurately reflect our approach in integrating Information Technology solutions into the organization's business processes using the advantage provided though the use of network metrics. This is a structured engineering process that assists our teams in determining system requirements and selecting technology necessary to support those requirements.

ADVANETRIX has demonstrated success at providing IT solutions that support the organization at all levels (Management, Network Engineers, and Users).

- **Woman-Owned Small Business**
- **Founded in 1997 in State of Virginia**
- **Headquarters located in Woodbridge, Virginia**
- **Participant in the National Industrial Security Program**
- **Established Infrastructure and Mature Program Management organization**
- **GSA Schedule - GS-35F0646N**
- **Participating in Small Business Association Exchange program which allows acquisitions up to $100,000.**
- **Established Solid Business Partners, Subcontractors, and Consultants**
- **Demonstrated Performance**

Mission Statement

Mission

The mission of ***ADVANETRIX*** is to provide the Federal Government and Commercial Customers with the highest quality Management Consulting and Information Technology Solutions.

Vision

Our vision is to continue to be a leading provider of proven solutions to our customers in the Federal and commercial marketplace. We will continually build on our solid foundation of recognized technical expertise, creating a hallmark staff of technical experts who are recognized throughout the information technology industry who are well-versed in all aspects of Government solutions. Recognizing the dynamic nature of today's information, we will identify and become knowledgeable in leading-edge technologies, enabling us to confidently respond to all of our customer's needs

Values

We will maintain integrity in all business transactions. We will nurture a working environment where all employees are treated with honesty and respect and are encouraged to grow and advance in their careers, personal development and involvement in the community.

Why You Should Choose ADVANETRIX

ADVANETRIX teams integrate skills in **Information Assurance**, **IT Engineering & Analysis**, and **Knowledge Management** to provide solutions that ensure that the appropriate security objectives are developed, security risks are identified and balanced against operational requirements in the development, deployment, maintenance, and assessment of systems and applications.

Our IT Engineering & Analysis Team provides network engineering, systems development and systems analysis teams that have a wide-range of skills that support Planning, Deploying/Integrating, Maintaining, Managing and Analyzing IT systems that support decision makers. Our commercial focus is on Microsoft software and DELL systems. Our DoD support is focused on Command, Control, Communications, Computers and Intelligence (C^4I) systems.

Our Knowledge Management Team provides integrated tools to support the management of our programs and to assist our customers in tailored solutions to meet their management needs.

ADVANETRIX works with its employees to establish a professional improvement plan that integrates our employees' education, certification and work experience with our corporate vision and future objectives. This process ensures that our professional workforce is highly qualified in areas relevant to our customer base and allows the corporation to accurately project its current and future capabilities and thereby controlling costs. Our professional improvement plan includes Training, Education and Certification.

- **ADVANETRIX** team **Integrates Skills** in Information Assurance; IT Engineering and Analysis; and Knowledge Management to provide a **complete solution** that considers the appropriate mix of people, process, technology and security.

- We employ **Standardized and Disciplined Processes** for the development of information technology solutions that balance cost, schedule, performance and risk.

- Our solutions are based upon " **Best Practices**" that are continuously updated**.**

- Our staff has **Proven Skills** that are continuously updated

- We have **Proven Performance** in support of IA, IT Engineering & Analysis, and Knowledge Management projects for organizations of Various Sizes, Complexity, and Diversity.

- We develop **Scalable, Reliable, Available, Secure**, and **Adaptable** solutions so that our customer's investment will support the organizations long-term objectives.

- **Quality** is our Standard

- **Customer Satisfaction** is our Measure of Effectiveness

Information Assurance (IA)

Information Assurance is defined as “ Information Operations (IO) that protect and defend information and information systems by ensuring their **availability, integrity, authentication, confidentiality**, and **non-repudiation**. This includes providing for restoration of information systems by incorporating **protection, detection**, and **reaction** capabilities”.

All organizations of any size or operating purpose has a need for the application of IA support to some degree. The need to protect information comes from many requirements to include legal obligations for privacy, contractual obligations to protect corporate information, financial liability and protection of critical assets.

The need is not uniform , because the risk to exposure is not uniform. The implementation strategy requires the consideration of People, Processes, Technology, organizations mission,

The results of many surveys have clearly articulated that the stakes involved in Information Assurance have risen. Your organization is vulnerable to numerous attacks from many different sources and the results can be devastating in terms of lost assets, compromised customer data, and inability to continue business operations.

Best practices, procedures templates and tools are being developed to help with IA assessment and implementation, but since no security solution is standard across any marketplace, the team that uses those tools must have an in-depth knowledge of the requisite security disciplines.

ADVANETRIX provides a team that is task-organized to meet the particular needs of our customers.

- **Enterprise Security Program Development, Assessment and Deficiency Remediation**
- **Certification and Accreditation**

  DOD Information Technology Security Certification & Accreditation Process (DITSCAP)

  National Information Assurance Certification & Accreditation Process (NIACAP)
- **Federal Information Security Management Act 2002 Support**
- **Clinger-Cohen Support**
- **Security Assessments**

IA – Enterprise Security Program Development

Enterprise Security Program Development. Managing security at multiple levels brings many benefits. Each level contributes to the overall computer security program with different types of expertise, authority and resources. The integration of management, operational and technical controls provides a "Defense-In-Depth" approach.

Management Controls. "Security topics that can be characterized as Managerial. They are techniques and concerns that are normally addressed by management in the organization's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization."

Operational Controls. "Security controls that focus on controls that are, broadly speaking, implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

Technical Controls. "Focuses on security controls that the computer system executes. These controls are dependent upon the proper functioning of the system for their effectiveness. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the organization."

➢Enterprise Security Program Development (Management, Operational and Technical Controls)

Management Controls

Risk Management
Review of Security Controls
Life-cycle Management (Vulnerabilities, etc)
Certification & Accreditation
System Security Plans Policies, Procedures Standards, & Guidance
Performance Metrics

Operational Controls

Personnel Security
Physical and Environmental
Production Input/Output Controls
Contingency Planning
Hardware & Software Maintenance
Data Integrity
Documentation(Architecture, User Guides,)
Security Awareness, Education & Training
Continuity Of Operations / Disaster Recovery Programs
Incident Response Support

Technical Controls

Identification and Authentication
Logical Access Controls
Audit Trails
Firewalls

IA – Certification & Accreditation

Certification and Accreditation. Office of Management and Budget Circular A-130, Management of Federal Information Resources requires federal agencies to plan for security, ensure that appropriate officials are assigned security responsibility, and authorize system processing prior to operations and, periodically thereafter. This authorization by senior agency officials is sometimes referred to as *accreditation.* The technical and non-technical (based upon Management, Operation and Technical Controls) evaluation of an IT system that produces the necessary information required by the authorizing official to make a credible, risk-based decision on whether to place the system into operation is known as *certification*.

DoD Information Technology Security Certification and Accredita6ion Process (DITSCAP). The DITSCAP defines a process that standardizes all activities leading to a successful accreditation. The principal purpose of that process is to protect and secure the entities comprising the Defense Information Infrastructure. Standardizing the process minimizes risks associated with nonstandard security implementations across shared infrastructure and end systems.

National Information Assurance Certification and Accreditation Process (NIACAP). "Establishes the minimum national standards for certifying and accrediting national security systems. This process provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the IA and security posture of a system or site. The process focuses on an enterprise-wide view of the information systems (IS) in relation to the organization's mission and the IS business case."

➢Basic Process

Phase 1: Definition

Focused on understanding the IS business case, environment, and architecture to determine the security requirements and level of effort necessary to achieve certification and accreditation. Objective – Agree on the security requirements, C&A boundary, schedule, level of effort, and resources required

Phase 2: Verification

Verifies the evolving or modified system's compliance with the information in the System Security Authorization Agreement (SSAA). Objective – Ensure the fully integrated system will be ready for certification testing.

Phase 3: Validation

Validates compliance of the fully integrated system with the security policy and requirements stated in the SSAA. Objective – To produce the required evidence to support the Designated Approval Authority (DAA) in making an informed decision to grant approval to operate the system (Full Accreditation), Interim Authority to Operate (Interim Accreditation), or Accreditation Disapproval.

Elements of Certification Package

•Security Plan
•Security Test & Evaluation Reports
•Final Risk Assessment Report
•Certifier's Statement

Elements of Accreditation Package

•Accreditation Letter
•Security Plan
•Report Documenting the Basis for the Accreditation Decision

Phase 4: Post Accreditation

Includes the activities necessary for the continuing operation of the Fully Accredited IS I its computing environment and to address the changing threats and small scale changes that a systems faces throughout its life cycle. Objective – Ensure secure system management, operation, and maintenance to preserve an acceptable level of residual risk.

Federal Information Security Management Act (FISMA) of 2002.

"The President has given a high priority to the security of the Federal Government's operations and assets. Protecting the information and information systems on which the Federal Government depends, requires agencies to identify and resolve current security weaknesses and risks, as well as protect against future vulnerabilities and threats. " The key method for fulfilling these requirements was the Government Information Security Act of 2000. In 2002, FISMA replaced GISRA.

FISMA establishes requirements that must be accomplished by all Federal Government Agencies. Four of those key requirements are outlined below. Completing the tasks to support FISMA requires the dedication of highly experienced IA professionals that posses an in-depth understanding of all elements of an effective and efficient security Program.

ADVANETRIX integrates expertise in Information Assurance; Information Technology Engineering and Analysis; and Knowledge Management to provide our customers with a team that has extensive experience in security program development, assessment and deficiency remediation. Our team includes members that have managed government security programs as Federal employees with specific experience in developing the products required for GISRA (now FISMA). We have additional capabilities to support other relevant areas such as in the Certification and Accreditation of information systems. Advanetrix is prepared to support your needs, please contact us or visit our internet site.

- **Develop an Agency-Wide Information Systems Security Program (ISP)**

  Periodic Assessment of Risks
  Plans for Information Systems Security for Networks, Facilities, and Systems.
  Security Awareness Training
  Periodic Testing and Evaluation of ISP
  Deficiency Remediation
  Incident Detection, Response and Reporting
  Continuity of Operations

- **Annual Independent Evaluation**

  Test the Effectiveness of: Policies, Procedures and Practices on a representative subset of Information Systems

- **Annual Report to Congress**

  Adequacy, Effectiveness and Compliance of Information Systems Security Policies and Practices
  Adequacy, and Effectiveness in Plans and Reports relating to Budgets, Financial Systems, and Internal Accounting and Administrative Controls Deficiencies

IT Engineering & Analysis

ADVANETRIX understands that Agencies buy information technology resources (computers and related products and services) to solve mission-critical problems and that investments in information technology (IT) can have a dramatic impact on an organization's performance. Well-managed IT investments that are carefully selected and focused on meeting mission needs can propel an organization forward, dramatically improving performance while reducing costs. Likewise, poor investments, those that are inadequately justified or whose costs, risks, and benefits are poorly managed, can hinder and even restrict an organization's performance.

At **ADVANETRIX**, our IT Engineers employ standardized and disciplined processes for the development of Information Technology solutions that balance cost, schedule, performance and risk. Additionally, we have demonstrated success with the application of all the skills necessary to perform the tasks indicated in the areas that we support. We have supported a full range of customers from DoD, Federal Agencies, and commercial corporations that have significantly different missions, organizations and business processes.

➢Plan

Operational, Systems And Technical Architecture Development
Process Engineering / Re-Engineering
Active Directory Design
Strategic Planning
Mission and Business Planning (define the need and intended Use)
Acquisition Planning

➢Deploy / Integrate / Migrate

Integration of Microsoft Products
System Migration
System Integration

➢Maintain / Manage

Seat Management
Performance Metrics
Life Cycle Management
IT Investment Management Planning
Clinger-Cohen Act of 1996
Change Management

➢Analyze

Requirements Analysis
Alternative Analysis
System Performance

Knowledge Management

Knowledge management consists of three fundamental components: **people, processes** and **technology**. Knowledge management focuses on people and organizational culture to stimulate and nurture the sharing and use of knowledge; on processes or methods to find, create, capture and share knowledge; and on technology to store and make knowledge accessible and to allow people to work together without being together.

Efficiencies occur when the right knowledge gets to the right people at the right time. KM is the conscious strategy of putting knowledge into action as a means to increase organizational performance.

Technology provides the means for people to organize, store and access explicit knowledge. It also provides the means for people to directly share their tacit knowledge without being face to face. Technology produces value when it increases the accessibility of knowledge, reduces the time and effort of employees to record and keep it current and facilitate interaction with citizens, customers, suppliers, partners and each other. (CIO Council)

- ➢**Web-Based Solutions**
- ➢**Targeted Database Development**
- ➢**Integration of Microsoft Components to Allow Document Management, Version Control, Search, and Collaboration Within the Enterprise**

WELCOME TO THE U.S. DEPARTMENT OF STATE POEMS WEBSITE
Marine Executive Association
Marines Helping Marines
Target on Y2K
Air National Guard

Quality Control Program

ADVANETRIX is committed to providing superior product and service quality by forming a partnership with its customers and team members, thus creating trust by establishing and communicating mutual expectations.

At ***ADVANETRIX***, our IT Engineers employ standardized and disciplined processes for the development of Information Technology solutions that balance cost, schedule, performance and risk. Additionally, we have demonstrated success with the application of all the skills necessary to perform the tasks indicated in the areas that we support. We have supported a full range of customers from DoD, Federal Agencies, and commercial corporations that have significantly different missions, organizations and business processes.

- On-Site Computer Lab Facilities
  - Standardize Training
  - Test technologies prior to implementation
  - Analyze security implications
- Automated Research Library
- Automated Document Management With Version and Approval Control
- Continuous Employee Education, Training and Certification Program
- Focus on Best Practices
- Periodic Quality Re-Evaluation (Close Coordination with Customer)

Information Assurance

✓Conducted Information Assurance Analysis for Logistics that was Linked to Combat Effectiveness

✓Developed Security Policy, Guidance and Procedures

✓Developed IA Strategy, Business Continuity Planning and Disaster Recovery Planning Documentation

✓Developed Documents to Support DoD Information Technology Security Certification & Accreditation Process (DITSCAP) for Existing Systems and Systems within the Acquisition Process

✓Evaluated Existing User Business Processes and Developed and Implemented Security Solutions

✓Assisted in the Development and management of Enterprise Information Security Program

✓Monitored Intrusion Detection System and Recommended Appropriate actions

✓Implemented Technology : Firewall, SSL, Virtual Private Networks, System Security Policy, ETC.

Information Technology Engineering & Analysis

✓Developed Information Exchange Requirements in Support of the Analysis of UAV, Satellite and Tactical Communication Systems to Support the Warfighter Information Architecture

✓Developed Activity Models and Information Flow Models for USMC Theater Missile Defense

✓Developed Information Exchange Requirements for Logistics Threads from Strategic to Tactical level

✓Migrated Information Enterprise (s) Operating Systems and Implemented Active Directory

✓Analyzed C^4I System Requirements and Implementation

✓Analyzed the Marine Corps Tactical Information Architecture to Include "Network Centric" Operations

✓Analyzed Information Requirements and Implemented System, Software and Security architectures

✓Analyzed Wireless Architecture required to support Network-Centric Warfare / Knowledge Management

✓Supported Development of C2 System Specification

Knowledge Management

✓Developed Data Bases to Provide Document Management, Reference Management, and to Support Specific Analysis Requirements of the Customer

✓Developed Web Sites to support Classified and Unclassified Networks

✓Analyzed Nine Combatant Commander’s Collaborative Information Environment

✓Developed Web-Site to support Information Assurance Program Management

✓Developed Database to support IA management

✓Integrated Live feeds into Browser-based Knowledge Management System

✓ Integrated Time Management, Financial Software, Document Management, and Other Business Software into a Knowledge Management System

✓Implemented SharePoint Intranets and Portal Solution and Microsoft Exchange

Scalable Support

Customers

- Department of Veteran’s Affairs
- Department of State
- OSD, C4ISR Decision Support Center
- Joint Chiefs of Staff, J6
- Army Materiel Command
- Army Logistics Integration Agency
- United States Marine Corps
- Space and Naval Warfare Systems Command
- Air National Guard
- Science and Regulatory Consultants, Inc.
- Eagan, McAllister Associates, Inc
- Ocean Systems Engineering Corporation
- FCI Incorporated
- Anteon Corporation

Partners

- Microsoft Corporation
- Dell
- Anteon Corporation
- Ocean Systems Engineering Corporation
- Alpha Informatics, Inc.

Contracts

INFORMATION ASSURANCE SECTION
Information Assurance Engineer I
Information Assurance Engineer II
Information Assurance Engineer III
Information Assurance Engineer IV
Information Assurance Engineer V
Information Assurance Engineer VI
Information Assurance Engineer VII
Information Assurance Engineer VIII
Information Assurance Engineer IX
Information Assurance Engineer X

INFORMATION TECHNOLOGY ENGINEERING & ANALYSIS SECTION
Network Engineer I
Network Engineer II
Network Engineer III
Network Engineer IV
Network Engineer V
Network Engineer VI
Information Technology Engineer I
Information Technology Engineer II
Information Systems Analyst I
Information Systems Analyst II
Information Systems Analyst III

PROGRAM SUPPORT SECTION
Program Director
Program Manager
Project Manager
Task Team Leader
Technical Writer
Quality Assurance Specialist

GSA Schedule
Contract GS-35F-0646N

KNOWLEDGE MANAGEMENT SECTION
Knowledge Management Specialist I
Knowledge Management Specialist II
Knowledge Management Specialist III
Knowledge Management Specialist IV

CONSULTING SECTION
Consultant I
Consultant II
Consultant III

For specific information pertaining to labor categories (minimum education, functional responsibility, minimum experience and rates) and contracting information, please see the Approved Advanetrix Price List

Contact Us

- Information Assurance
- IT Engineering & Analysis
- Knowledge Management

Mike Lewis
mlewis@advanetrix.com
CEO

P (703) 492-1782 Ext 12
F (703) 492-7565

ADVANETRIX, INC.
12724 Director’s Loop
Woodbridge, VA 22192